UTHSC G.U.A.R.D.

February 2017

IN THIS ISSUE

The Importance of Data Encryption

by Uneice Alexander, UTHSC Information Security Team Intern

Encryption is a process that scrambles data into cyphertext, so anyone trying to read the data finds nothing more than gibberish. When talking about encryption, it is significant to be aware of the distinction that all modern encryption technology is derived from cryptography. Cryptography is the act of creating and (attempting to) decipher a code. While electronic encryption is relatively new in the grander scheme of things, cryptography existed as far back as ancient Greece.

Spartan generals sending and receiving sensitive messages would wrap a piece of parchment around an instrument used as a tool to create encrypted messages as a means of keeping information secret. When someone removed the paper from the cylinder, the writing appeared to be a jumble of nonsense. The other general receiving the message could wrap a parchment of similar size around it, and easily read the intended message.

We have entered a time when the conveniences of widespread connectivity can provide everyone the flexibility of carrying a networked device on his or her person. A study conducted by the Ponemon Institute indicated, "two out of three lost smartphones contained sensitive or confidential business information", which makes mobile device encryption especially important. The incredible growth of connectivity has excited businesses and consumers alike with its promise of changing the way we live and work. It has also put us at more risk than ever of being hacked.

Data security is a major concern, especially when you are sending sensitive information. Encryption is a great way to keep valuable data safe, making it completely unreadable to anyone but you or its intended recipient. Whether you are transmitting it over the Internet, or just carrying it through airport security on your laptop. Encryption makes the ability to securely store or send personal and private information possible while protecting individual privacy and business information from exploitation.

Why Encrypt?

Learn about the history and importance of encryption.

Security Breaches are Everyone's Business

See what cyber security breaches can actually mean.

Why Should You Be Concerned about Cyber Security Breaches?

by Uneice Alexander, UTHSC Information Security Team Intern

Cyber-security should be everyone's concern. Data theft has become a global phenomenon. Public and private entities in the U.S. are overwhelmingly the most attractive targets of cyber-attacks. Over two billion records were stolen in 2016 alone. It is difficult for any entity to eliminate the possibility of being vulnerable when it comes to cyber-attacks. Successful and notable cyber incidents hardly scratch the surface of the number of attacks or breaches that occur daily. Hackers constantly continue to target large databases, as well as point-of-sale systems, for financial gain.

These attacks underline the fact that criminals will exploit any vulnerability in any system. It also highlights the fact that no sector can consider itself immune to attack and must constantly address their security procedures to better protect themselves from these evolving threats.

Data stolen from a bank quickly becomes useless once the breach is discovered and passcodes are changed. But data from the healthcare industry, which includes both personal identities and medical histories, can live a lifetime.

The Ponemon report "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data" by the Ponemon Institute estimates that data breaches cost the healthcare industry some $6.2 billion.

Alliance Health's online portal that facilitates support and information communities across health providers may have exposed personal health information of its 1.5 million users. Forty thousand individuals were eventually informed their information had been exposed for 30 months.

Banner Health's almost four million patients, physicians, and customers were affected. The breach was first noticed on July 7, 2016, affecting payment card information. A subsequent breach led to the unauthorized access of patients' personal identifiable information, such as birthdates, claims information, and possibly social security numbers.

Research demonstrates that the healthcare sector is uniquely vulnerable to privacy breaches due to regulations for healthcare operations to adopt electronic health records (EHR). Healthcare records contain some of the most valuable information available, including Social Security numbers, home addresses and patient health histories, making them more valuable to hackers than other types of data.

All it takes is opening up an email attachment for hackers to gain access to hospital systems. Despite the potential threats that malicious actors may pose to online network systems, the Internet and electronic devices continue to drive the economies of the world. We should take cybersecurity seriously while allowing innovation to continue to thrive. Security is everybody's business. It is not just up to the IT department. For more information, contact the Information Security team at 901-448-1579 or itsecurity@uthsc.edu.